보안 방화벽 위협 방어의 VRF(Virtual Router) 이해

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[라이센싱](#)
[사용되는 구성 요소](#)
[배경 정보](#)
[기능 개요](#)
[VRF 지원](#)
[라우팅 정책](#)
[중복 네트워크](#)
[설정](#)
[FMC](#)
[FDM](#)
[REST API](#)
[FMC](#)
[FDM](#)
[활용 사례](#)
[통신 사업자](#)
[리소스 공유](#)
[호스트와의 중첩 네트워크가 서로 통신함](#)
[BGP 경로 유출](#)
[확인](#)
[문제 해결](#)
[관련 링크](#)

소개

이 문서에서는 **Virtual Routing and Forwarding (VRF)** Cisco FTD(**Secure Firewall Threat Defense)의 기능 입니다**.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco **Secure Firewall Threat Defense (FTD)FTD(보안 방화벽 위협 방어)**
- **Virtual Routing and Forwarding (VRF)**
- 동적 라우팅 프로토콜(OSPF, BGP)

라이센싱

특정 라이센스 요구 사항이 없습니다. 기본 라이센스면 충분합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco **Secure Firewall Threat Defense (FTD), Secure Firewall Management Center (FMC)** 버전 7.2.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 **Virtual Routing and Forwarding (VRF)** ftd 소프트웨어 릴리스 6.6에 기능이 추가되었습니다.

이 기능은 다음과 같은 장점을 제공합니다.

- 라우팅 테이블 분리
- IP 주소 공간에서 겹치는 네트워크 세그먼트
- VRF 라이트
- 다중 컨텍스트 마이그레이션 활용 사례에 대한 FXOS 다중 인스턴스 지원
- BGP **Route Leak Support-v4v6** 및 BGPv6 **VTI Support** ftd 소프트웨어 릴리스 7.1에 기능이 추가되었습니다.

기능 개요

VRF 지원

디바이스	최대 가상 라우터
ASA	10-20
Firepower 1000*	5-10 *1010(7.2+)
Firepower 2100	10-40
Firepower 3100	15-100
Firepower 4100	60-100
Firepower 9300	60-100
가상 FTD	30
ISA 3000	10(7.0+)

기본 모드의 블레이드당 VRF 제한

라우팅 정책

정책	글로벌 VRF	사용자 VRF
고정 경로	✓	✓
OSPPFv2	✓	✓
OSPFv3	✓	✖
RIP	✓	✖

BGPv4	✓	✓
BGPv6	✓	✓(7.1+)
IRB(BVI)	✓	✓
EIGRP	✓	✖

중복 네트워크

정책	비중첩	중복 네트워크
라우팅 및 IRB	✓	✓
AVC	✓	✓
SSL 암호 해독	✓	✓
침입 및 악성코드 탐지(IPS 및 파일 정책)	✓	✓
VPN	✓	✓
악성코드 이벤트 분석(호스트 프로필, IoC, 파일 전파 흔적 분석)	✓	✖
위협 인텔리전스(TID)	✓	✖

설정

FMC

1단계. 탐색 **Devices > Device Management** 을 누르고 구성할 FTD를 편집합니다.

2단계. 탭으로 이동합니다. **Routing**

3단계. 클릭 **Manage Virtual Routers .**

4단계. 클릭 **Add Virtual Router .**

5단계. Add Virtual Router(가상 라우터 추가) 상자에 가상 라우터의 이름과 설명을 입력합니다.

6단계. 클릭 **Ok .**

7단계. 인터페이스를 추가하려면 **Available Interfaces** 상자를 클릭한 다음 **Add .**

8단계. 가상 라우터에서 라우팅을 구성합니다.

- OSPF
- RIP
- BGP
- 정적 라우팅
- 멀티캐스트

FDM

1단계. 탐색 **Device > Routing .**

2단계.

- 생성된 가상 라우터가 없는 경우 **Add Multiple Virtual Routers** 를 클릭한 다음 **Create First Customer Virtual Router .**

- 가상 라우터 목록 상단의 **+** 버튼을 클릭하여 새 라우터를 생성합니다.

3단계. 의 **Add Virtual Router** 상자를 클릭합니다. 가상 라우터의 이름 및 설명을 입력합니다.

4단계. 가상 **라우터**에 포함되어야 하는 각 인터페이스를 선택하려면**+**를 클릭합니다.

5단계. 클릭 **Ok** .

6단계. 에서 라우팅 구성 **Virtual Router**.

- OSPF
- RIP
- BGP
- 정적 라우팅
- 멀티캐스트

REST API

FMC

FMC는 전체 CRUD 가상 라우터에 대한 작업입니다.

가상 라우터 호출의 경로는 **Devices > Routing > virtualrouters**

FDM

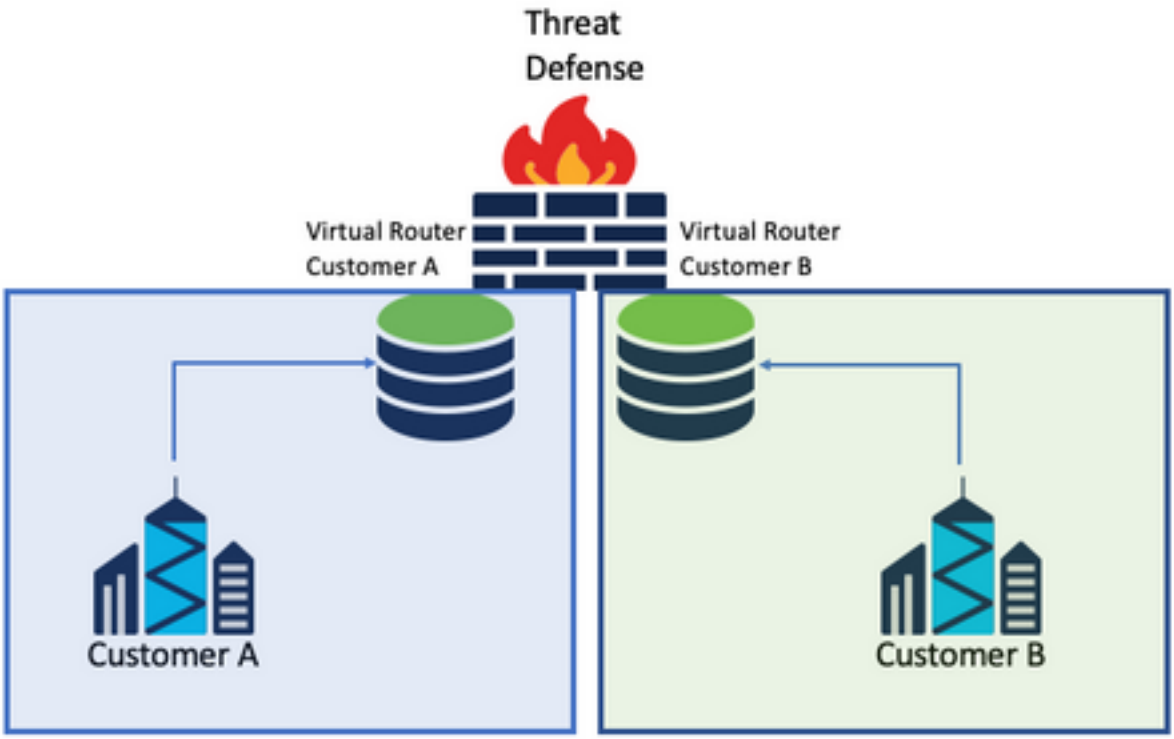
FDM은 가상 라우터에서 전체 CRUD 작업을 지원합니다.

가상 라우터 호출의 경로는 **Devices > Routing > virtualrouters**

활용 사례

통신 사업자

개별 라우팅 테이블에서 두 네트워크는 서로 관련이 없으며 서로 간의 통신이 없습니다.

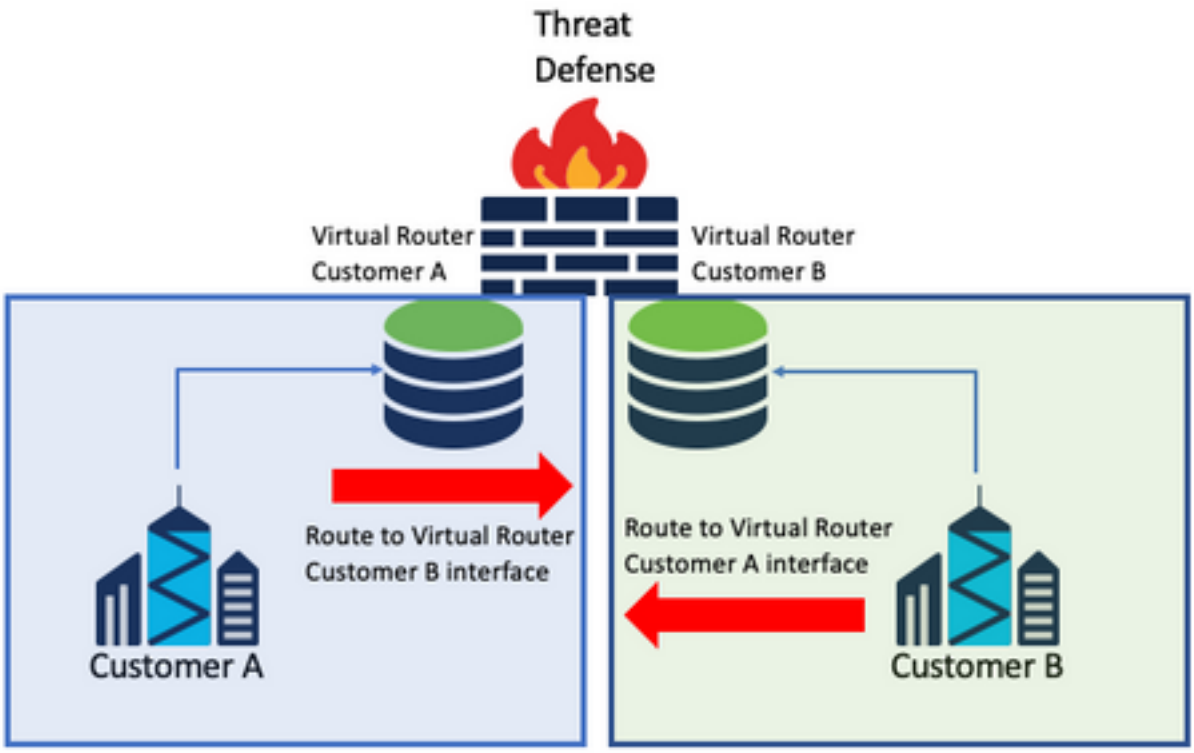


고려 사항:

- 이 시나리오에서는 특별한 고려 사항이 없습니다.

리소스 공유

두 개의 가상 라우터를 상호 연결하여 각 라우터의 리소스를 공유하고 **Customer A** 수신 **Customer B** 그리고 그 반대도 마찬가지입니다.



고려 사항:

- 각 가상 라우터에서 다른 가상 라우터의 인터페이스를 사용하여 대상 네트워크를 가리키는 고정 경로를 구성합니다.

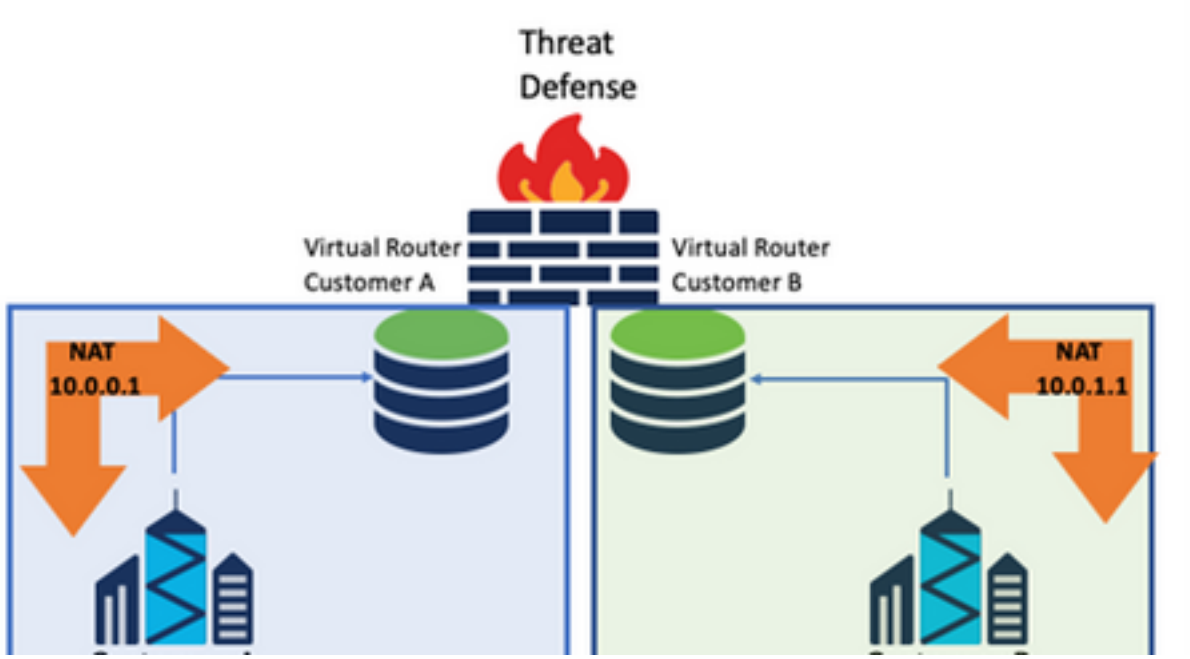
예:

가상 라우터에서 **Customer A**를 사용하여 경로를 목적지로 추가 **Customer B** 게이트웨이로서의 IP 주소가 없는 인터페이스(필요 없음, 다음과 같이 알려짐) **route leaking**).

에 대해 동일한 프로세스를 반복합니다. **Customer B.**

호스트와의 중첩 네트워크가 서로 통신함

동일한 네트워크 주소와 이들 간의 트래픽 교환이 가능한 2개의 가상 라우터가 있습니다.



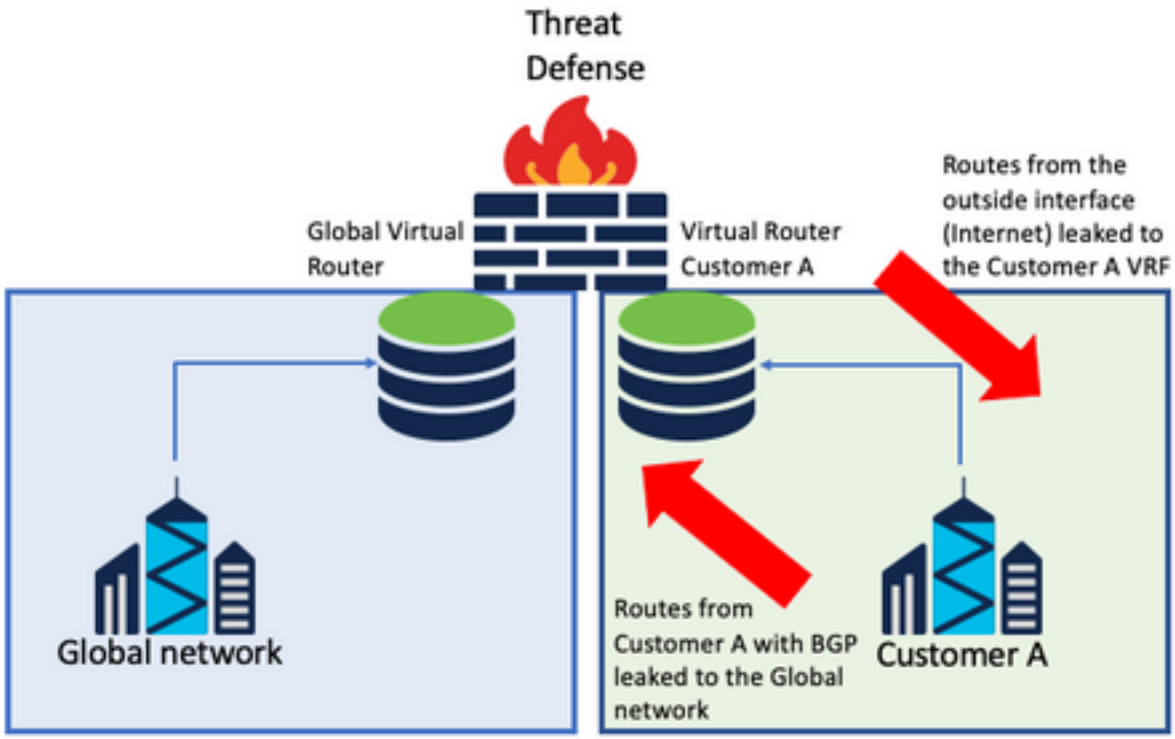
고려 사항:

두 네트워크 간에 통신을 수행하려면 소스 IP 주소를 재정의하고 위조 IP 주소를 넣도록 Twice NAT를 구성합니다.

BGP 경로 유출

사용자 정의 가상 라우터가 하나 있으며 해당 가상 라우터의 경로를 전역 가상 라우터로 유출해야 합니다.

외부 인터페이스는 전역 인터페이스에서 사용자 정의 가상 라우터로 유출되도록 라우팅합니다.



고려 사항:

- FTD 버전이 7.1 이상인지 확인합니다.
- 의 **가져오기/내보내기** 옵션을 사용합니다. **BGP > IPv4** 메뉴를 선택합니다.
- 배포에 경로 맵을 사용합니다.

확인

가상 라우터가 생성되었는지 확인하는 방법은 다음 명령을 사용합니다.

```
firepower# show vrf

Name                              VRF ID     Description     Interfaces
VRF_A                             1          VRF A               DMZ
firepower# show vrf detail

VRF Name: VRF_A; VRF id = 1 (0x1)
VRF VRF_A (VRF Id = 1);
  Description: This is VRF for customer A
  Interfaces:
    Gi0/2
Address family ipv4 (Table ID = 1 (0x1)):
  ...
Address family ipv6 (Table ID = 503316481 (0x1e000001)):
  ...

VRF Name: single_vf; VRF id = 0 (0x0)
VRF single_vf (VRF Id = 0);
  No interfaces
Address family ipv4 (Table ID = 65535 (0xffff)):
  ...
Address family ipv6 (Table ID = 65535 (0xffff)):
  ...
```

문제 해결

VRF에 대한 정보를 수집하고 진단하는 데 필요한 명령은 다음과 같습니다.

모든 VRF

- **show route all**
- **show asp table routing all**
- **packet tracer**

글로벌 VRF

- **show route**
- **show [bgp|ospf] [subcommands]**

사용자 정의 VRF

- **show route [bgp|ospf] vrf {name}**

관련 링크

Cisco Secure Firewall Management Center Device Configuration Guide, 7.2 - Virtual Routers
Cisco Secure Firewall Management Center - Cisco

Cisco Secure Firewall Device Manager 컨피그레이션 가이드, 버전 7.2 - 가상 라우터 Cisco Secure Firewall 위협 방어 - Cisco

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.